

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

LISTING OF CLAIMS:

1. (Currently Amended) A communication system in which an image processing apparatus ~~a device~~ and a client communicate data with each other through a network,

wherein said image processing apparatus ~~device~~ comprises:

a root certificate creator ~~first storage device~~ which creates ~~stores~~ a root certificate including a public key paired with a private key and being signed with the private key;

a second certificate creator which creates, when a connection for communication is requested by said client, a second certificate designating the root certificate created by said root certificate creator as a certificate authority at a higher level and being signed with the private key used to sign the root certificate; and

a communication device which transmits the second certificate created by said second certificate creator to said client; and

wherein said client comprises:

a ~~second~~ storage device which has stored therein, before the connection for communication is requested to said image processing apparatus ~~device~~, the root certificate created by said root certificate creator ~~stored in said first storage device~~; and

a verifier which verifies the signature of the second certificate received from said image processing apparatus device with the root certificate stored in said ~~second~~ storage device.

2. (Currently Amended) The communication system according to claim 1, wherein said image processing apparatus device is a printer.

3. (Currently Amended) The communication system according to claim 1, wherein said image processing apparatus device is a multifunctional peripheral.

4. (Original) The communication system according to claim 1, wherein said client is a personal computer.

5. (Currently Amended) The communication system according to claim 1, wherein said ~~second~~ storage device is a hard disk drive.

6. (Original) The communication system according to claim 1, wherein said second storage device is a read-only memory.

7. (Currently Amended) A communication method for a communication system in which ~~a device~~ an image processing apparatus and a client communicate data with each other through a network,

wherein the ~~device~~image processing apparatus creates ~~holds~~ a root certificate including a public key paired with a private key and being signed with the private key;

the client installs the root certificate which is ~~held in~~created by the device image processing apparatus and which includes the public key, prior to the client requesting a connection for communication to the ~~device~~image processing apparatus;

the ~~device~~image processing apparatus creates, when a connection for communication is requested by the client, a second certificate designating the root certificate created by the image processing apparatus as a certificate authority at a higher level and being signed with the private key used to sign the root certificate when data is sent to the client;

the ~~device~~image processing apparatus sends the second certificate to the client; and

the client verifies the signature of the second certificate received from the ~~device~~image processing apparatus with the installed root certificate.

8. (Currently Amended) The method according to claim 7, wherein the ~~device~~image processing apparatus further holds at least one intermediate certificate for one or more certificate authorities existing in a hierarchical order up to a root certificate authority;

the client installs the at least one intermediate certificate in addition to the root certificate;

the ~~device~~image processing apparatus sends the second certificate to the client; and

the client verifies the signature of the second certificate received from the ~~device~~image processing apparatus with the at least one intermediate certificate installed therein, and verifies the signature of the at least one intermediate certificate received from the ~~device~~image processing apparatus with the root certificate installed therein.

9. (Currently Amended) The method according to claim 7, wherein when the client installs the root certificate, the client requests the root certificate from the ~~device~~image processing apparatus when a printer driver from the ~~device~~image processing apparatus is installed in the client, receives the root certificate from the ~~device~~image processing apparatus, converts the received root certificate to a predetermined format when the root certificate is received, and installs the converted root certificate.

10. (Previously Presented) The method according to claim 7, wherein when the client installs the root certificate, the installation is performed after the root certificate is confirmed by a user.

11. (Currently Amended) The method according to claim 7, wherein the ~~device~~image processing apparatus is a printer, ~~has a print function~~, and the client installs the root certificate after a printer driver from the ~~device~~image processing apparatus is installed in the client.

12. (Previously Presented) The method according to claim 7, wherein the data is communicated according to the security sockets layer (SSL) protocol.

13-16. (Cancelled)

17. (Currently Amended) ~~A device~~ An image processing apparatus to be used in a communication system in which the ~~device~~ image processing apparatus and a client communicate with each other through a network, the ~~device~~ image processing apparatus sends information to the client, and the client uses the information to communicate with the ~~device~~ image processing apparatus, the ~~device~~ image processing apparatus comprising:

a ~~first storage device~~ root certificate creator which ~~stores~~ creates a root certificate including a pair of a public key and paired with a private key and being signed with the private key;

a ~~second storage device~~ which stores a the root certificate signed with the private key;

a second certificate creator which creates, when a connection for communication is requested by the client, a second certificate designating the root certificate created by said root certificate creator as a certificate authority at a higher level and being signed with the private key used to sign the root certificate; and

an interface which sends the information as well as the root certificate including the public key to the client through the network before the connection for communication is requested to the ~~device~~ image processing apparatus, and sends,

after the root certificate created by said root certificate creator ~~stored in said second storage device~~ is installed in the client, the second certificate to the client for verification of the information sent from the ~~device~~ image processing apparatus.

18. (Currently Amended) The ~~device~~ image processing apparatus according to claim 17, wherein the ~~device~~ image processing apparatus is ~~a device which functions as a printer.~~

19. (Currently Amended) The ~~device~~ image processing apparatus according to claim 17, wherein the information is a printer driver.

20. (Currently Amended) The communication system according to claim 1, wherein the root certificate is stored in said first-storage device of said client ~~is stored in said second storage device~~ prior to the transmission of the second certificate to said client from said communication device.

21. (Cancelled)

22. (Currently Amended) The communication system according to claim 1, wherein said verifier is operable to verify the signature of the second certificate by decrypting the public key of the root certificate stored in said ~~second~~ storage device to obtain a first hash value, calculating a second hash value of the second certificate received from said ~~device~~ image processing apparatus, and comparing the first and second hash values to determine if they are equal to each other.

23. (Currently Amended) The method according to claim 7, wherein the ~~device~~image processing apparatus sends the second certificate to the client after the root certificate is installed in the client.

24. (Currently Amended) The method according to claim 8, wherein the client installs the at least one intermediate certificate prior to receiving the second certificate from the ~~device~~image processing apparatus.

25-27. (Cancelled)

28. (Currently Amended) The communication system according to claim 1, wherein:

the ~~second~~ storage device of said client has stored therein, before the connection for communication is requested to said ~~device~~image processing apparatus, the public key of the root certificate; ~~stored in said first storage device~~; and

the verifier verifies the signature of the second certificate received from said ~~device~~image processing apparatus by decrypting the second certificate with the public key of the root certificate stored in said ~~second~~ storage device of said client.

29. (Currently Amended) The communication method according to claim 7, wherein:

the client stores the public key of the installed root certificate, prior to the client requesting the connection for communication to the ~~device~~image processing apparatus; and

the client verifies the signature of the second certificate received from the device by decrypting the second certificate with the public key of the root certificate stored in the client.

30. (Cancelled)

31. (Currently Amended) A computer-readable recording medium having a computer program recorded thereon for causing a computing device, which is communicatively coupled to the computer-readable recording medium and which is configured to communicate with a client through a network to send information to the client, which uses the information to communicate with the computing device, to perform operations comprising:

storing a pair of a public key and a private key;

creating a root certificate including the public key and private key and being signed with the private key;

storing ~~a~~the root certificate signed with the private key;

sending the information and the root certificate created by the computing device and including the public key to the client, before a request for communication is requested by the client;

creating, when the connection for communication is requested by the client, a second certificate designating the root certificate created by the computing device as

a certificate authority at a higher level and being signed with the private key used to sign the root certificate; and

sending, after the root certificate has been installed in the client, the created second certificate to the client for verification of the information sent from the computing device.

32. (Currently Amended) The computer-readable recording medium according to claim 31, wherein the computing device is ~~a device which functions as a~~ printer.

33. (Previously Presented) The computer-readable recording medium according to claim 31, wherein the information is a printer driver.